UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
One LG smartphone and one Samsung Android smartphone, currently in the possession of the FBI, 600 Arch St., Philadelphia, PA

Case No. 20-85-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

One LG smartphone and one Samsung Android smartphone further described in Attachment A

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence, contraband, fruits and instrumentalities of a crime, further described in Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1591	sex trafficking of a minor
18 USC 2251, 2252	production and possession of child pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA Meaghan Moody

Printed name and title

Sworn to before me and signed in my presence.

Date: 1/22/2020

Judge's signature

City and state: Philadelphia, PA

Hon. Lynne A. Sitarski, U.S. Magistrate

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Meagan M. Moody, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Philadelphia Division, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI since July 2018, and am currently assigned to the Philadelphia Division's Violent Crimes Against Children Squad, which investigates sex trafficking and child pornography, among other violations of federal law. I have gained experience through training at the FBI Academy and everyday work related to conducting these types of investigations.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant to search: (a) one LG smartphone, model number LG-TP450, Serial Number 706CYEA177228, IMEI 357016-08-177228-2; and (b) one Samsung Android smartphone, Model Number SM-S550TL, Serial number RV8HC0LPRWZ, IMEI 359578071862439; (together, the SUBJECT PHONES), further described in Attachment A, for evidence, contraband and instrumentalities, further described in Attachment B, of violations of Title 18, United States Code, Section 1591, sex trafficking of a minor, Section 2251, production of child pornography, and Section 2252, possession of child pornography.

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I

believe are necessary to establish probable cause to believe that evidence of violations of Title 18 U.S.C. Sections 1591, 2251 and 2252 will be located on the SUBJECT PHONES.

LEGAL AUTHORITY

5. Title 18, United States Code, Section 1591 makes it a crime to recruit, entice, harbor, transport, provide, obtain, advertise, maintain, patronize, or solicit by any means a person, or to benefit, financially or by receiving anything of value, from participating in such a venture, knowing or in reckless disregard of the fact that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act.

6. Title 18, United States Code, Section 2251, makes it a crime to employ, use, persuade, induce, entice or coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of that conduct, where the visual depiction was produced or transmitted using materials that have been transported in or affecting interstate or foreign commerce. Sexually explicit conduct is defined under Title 18, United States Code, Section 2256(2) to include the lascivious exhibition of the genitals or pubic area of any person.

7. Title 18, United States Code, Section 2252(a)(4)(B) makes it a crime to knowingly possess any matter which contains a visual depiction of a minor that was produced using materials that were transported in interstate or foreign commerce, where the visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction was of such conduct.

BACKGROUND OF THE INVESTIGATION

8. On March 15, 2018, VICTOR CLAYTON, date of birth November xx, 1974, was arrested by the Dunn Police Department (DPD) in Harnett County, North Carolina for sex offenses against a minor, after DPD received a call regarding a missing juvenile possibly

involved in solicitation. DPD seized four phones at the time of CLAYTON's arrest from Room 214, Baymont Inn, 901 Jackson Road, Dunn, North Carolina, where CLAYTON was staying with two minor females. These four phones included: (a) a Blue/grey LG smartphone with a cracked screen (a SUBJECT PHONE); (b) a Black Samsung smartphone (a SUBJECT PHONE); (c) a Black iPhone with cracked screen in black "ThugLife" case; and (d) an iPhone in white-edged case.

9. Following CLAYTON's arrest, an FBI Special Agent from the FBI Charlotte, Raleigh Resident Agency interviewed the two minors, Minor 1 and Minor 2, who had been at the hotel with CLAYTON. Subsequently, FBI Special Agent Glenn Booth from the FBI Philadelphia office interviewed the same minor victims on multiple occasions.

10. Minor 1 advised that, beginning in roughly February 2018, CLAYTON had caused her to engage in prostitution along with other girls at a Motel 6 located at 11580 Roosevelt Boulevard, Philadelphia, Pennsylvania. CLAYTON booked the hotel through the internet website Booking.com. The first night in the Motel 6, Minor 1 had sex with two to three sex buyers. When she finished with each sex buyer, CLAYTON came back to the room and collected half of the money. CLAYTON also caused the girls to prostitute at the American Motor Inn, located at 4444 City Avenue, Philadelphia, Pennsylvania, and the Days Inn, located at 4200 East Roosevelt Boulevard, Philadelphia, Pennsylvania.

11. Minor 1 stated that CLAYTON utilized two android cell phones. CLAYTON posted advertisements for Minor 1 and the other girls on Backpage.com, a well-known Internet website for advertising prostitution, which allows users to post an advertisement for a fee. CLAYTON told the girls how to pose, and took pictures of the girls utilizing the SUBJECT PHONES which he used in their Backpage advertisements. CLAYTON also took nude

photographs of Minor 1 utilizing a SUBJECT PHONE. Minor 1 told CLAYTON she was sixteen years old in February 2018, so CLAYTON knew that Minor 1 was sixteen years old, and told her to tell people that she was nineteen and from New Jersey.

12. An FBI search of Backpage.com revealed numerous advertisements for sex with minors working for CLAYTON, including advertisements containing photographs of Minor 1, which Minor 1 identified. CLAYTON told Minor 1 he posted the advertisements regularly to ensure the advertisements were listed first on Backpage. Based on my training and experience, I know that Backpage advertisements can be posted from cellular phones.

13. Minor 1 advised that on approximately March 12 or 13, 2018, CLAYTON drove Minor 1 to pick up her friend, Minor 2, and that CLAYTON later took Minor 1 and Minor 2 to North Carolina.

14. Minor 2 told the FBI that she was from Pennsylvania, and that CLAYTON and Minor 1 picked her up in a vehicle in March 2018, advised her that they were going to advertise her on Backpage.com, and told her that she was expected to have sex with sex buyers. After the three of them spent the night together in Northeast Philadelphia, on March 13, 2018, CLAYTON drove Minor 1 and Minor 2 to North Carolina. Minor 2 was menstruating and told Clayton she could not have sex with sex buyers. Clayton said he still planned to post her on Backpage for oral sex.

15. On the drive to North Carolina, CLAYTON told Minor 1 to go on Backpage on one of the SUBJECT PHONEs and look up advertisements in North Carolina to see how much people were charging for commercial sexual encounters. CLAYTON utilized a SUBJECT PHONE to call multiple phone numbers from Backpage advertisements to ask about rates.

16. Minor 2 advised that CLAYTON checked in at the front desk of the Baymont Inn in Dunn, North Carolina. CLAYTON, Minor 1, and Minor 2, stayed in room 214 for two nights. Minor 1 confirmed that two of the four phones seized by DPD from room 214 were hers and two belonged to CLAYTON. Minor 1 used the two iPhones and CLAYTON used a grey Android phone and a second Android-type smart phone (the SUBJECT PHONES).

17. On April 12, 2018, the SUBJECT PHONES were transferred from the custody of DPD to FBI Philadelphia, and have remained in a locked evidence locker since that time.

18. On November 15, 2018, subject VICTOR CLAYTON was indicted by a Federal Grand Jury in the Eastern District of Pennsylvania on two counts of sex trafficking of a minor, in violation of 18 U.S.C. 1591. Trial is currently scheduled for March 30, 2020.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER/PHONE SYSTEMS

19. Searches and seizures of evidence from computer devices, cell phones, smart phones, and GPS's commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, cell phones, smart phones, GPS's, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take

days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer and electronic systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. In addition, there is probable cause to believe that these computer and electronic devices are all instrumentalities of the crime, within the meaning of Title 18 U.S.C. §§ 1591, 2251, and 2252, and should all be searched and seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

21. To search for electronic data contained in computer, including cell phone or electronic device hardware, computer, phone, or electronic device software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. searching for image files to locate images of children engaging in sexually explicit conduct, examining log files associated with the receipt, transmission, and viewing of

such images, and examining all of the data contained in such computer hardware, computer software, and /or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. surveying various file directories and the individual files they contain;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B;

g. searching for malware in order to evaluate defenses, such as viruses; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

ABILITY TO RETRIEVE DELETED FILES

22. Computer files or remnants of such files on traditional or conventional mechanical computer hard drives can typically be recovered months or even years after they

have been downloaded onto the hard drive, deleted or viewed via the Internet. Electronic files downloaded to the hard drive or storage device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files may reside in free space or slack space (that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space) for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from these conventional types of hard drives depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

23. Other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory based hard drives and devices. This technology has been traditionally used for small thumb drives where files and data are stored electronically, but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSD's and also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and

longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and overwritten. Because of how these flash memory-based drives function files may still be able to be recovered, however it may limit how much data, if any, can be recovered from these types of devices.

CONCLUSION

24. Based upon the information above, I respectfully submit that there is probable cause to believe that evidence, contraband and fruits and instrumentalities of violations of Title 18 U.S.C. Sections 1591, 2251 and 2252, further described in Attachment B, will be located on: a) one LG smartphone, model number LG-TP450, Serial Number 706CYEA177228, IMEI 357016-08-177228-2 and b) one Samsung Android smartphone, Model Number SM-S550TL, Serial number RV8HC0LPRWZ, IMEI 359578071862439, the SUBJECT PHONES, further described in Attachment A. Therefore, I respectfully request that the attached search warrant be issued.

Meagan M. Moody
Special Agent
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED
BEFORE ME THIS 22nd DAY
OF JANUARY, 2020.

Lynne A. Sitarski
HONORABLE LYNNE A. SITARSKI
United States Magistrate Judge

ATTACHMENT A

ITEM TO BE SEARCHED

1. One LG smartphone, model number LG-TP450, Serial Number 706CYEA177228, IMEI 357016-08-177228-2, currently in the possession of the FBI, 600 Arch Street, Philadelphia, Pennsylvania.
2. One Samsung Android smartphone, Model Number SM-S550TL, Serial number RV8HC0LPRWZ, IMEI 359578071862439, currently in the possession of the FBI, 600 Arch Street, Philadelphia, Pennsylvania.

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

Evidence of violations of 18 U.S.C. Sections 1591, 2251 and 2252, including the following:

1. All visual depictions of minors engaged in sexually explicit conduct, including those in opened or unopened e-mails or text messages. These include both originals and copies.

2. All records relating to prostitution, commercial sex, or the sex trafficking of minors, including stored communications, contact information, text messages, call logs, voicemails, Internet searches, Internet history, Internet advertisements, photographs, correspondence, chat logs, apps, and any other electronic data or other memory features contained in the devices.

3. All communications and records with or about potential minors engaging in commercial sex.

4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

5. All records bearing on the production or possession of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

6. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries,

reference materials, or other personal items, and registration information for any software on the computer or device.

7. All records regarding the ownership and/or possession of the searched items.

8. During the course of the search, photographs of the devices may also be taken to record the condition thereof and/or the location of items therein.

9. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

10. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any visual depictions described in paragraph 1 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.

The above seizure of computer, electronic device, and computer related hardware relates to such computer-related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting.